Perancangan Aplikasi Pengamanan Pesan E-mail Dengan Metode Kriptografi RSA Berbasis Android Studio

Rahadatul 'Aisy Riadi[1)], Ery Safrianti[2)], Linna Oktaviana Sari[3)]
[1)]Mahasiswa Program Studi Teknik Informatika, [2,3)]Dosen Teknik Informatika
Laboratorium Teknik Elektro Universitas Riau
Program Studi Teknik Informatika S1, Fakultas Teknik Universitas Riau
Kampus Bina Widya Jl. HR. Soebrantas Km. 12,5 Simpang Baru, Panam, Pekanbaru 28293
Email. rahadatul.aisyriadi@student.unri.ac.id

ABSTRACT

Communication is the most important part of everyday activities. In the current era, communication can be done in various ways. One of them is through electronic messages (E-mail). E-mail is a means of exchanging information through electronic communication by sending, receiving, changing and storing messages. Using e-mail is more practical than writing and sending letters manually. However, the use of email is also very vulnerable to crimes in electronic communication or the internet. Security and confidentiality issues are an important aspect of messages, data and information. This is related to the importance of messages and information sent and received by interested parties or people, whether the authenticity of the messages and information is still maintained or not. Therefore, security is needed to maintain the authenticity of messages or information from the contents of the e-mail using cryptography. Cryptography is the art and science of encryption that aims to maintain the security and confidentiality of data. In maintaining the confidentiality and security of electronic messages, the RSA (Revest Shamir Adleman) algorithm method is used, so that the confidentiality and security of the data or information can be maintained and RSA has security at the level of difficulty in factoring nonprime numbers. RSA has a key pair, namely a public key and a private key. This research produces an android application that aims to maintain the authenticity of message contents and information sent by means of messages that have been sent can only be read through the application. Messages sent through the application will also enter into Gmail's incoming contacts. But the user cannot read the message from Gmail because the contents of the message are encrypted and can only be read from the application. And users can only send messages to other users of the application.

Keywords: *Cryptography, RSA, Email, Android, Enkripsi. Deskripsi*

1. PENDAHULUAN

Komunikasi merupakan bagian terpenting dalam beraktivitas sehari-hari. Di era informasi ini komunikasi dapat dilakukan dengan berbagai cara. Salah satunya melalui pesan elektronik (email). Email merupakan suatu sarana pertukaran informasi melalui komunikasi elektronik dengan cara mengirim, menerima, mengubah dan menyimpan pesan (Lesmana dkk, 2018).

Penggunaan email dalam komunikasi surat menyurat jauh lebih praktis dibandingkan secara manual. Namun penggunaan email juga sangat rentan terhadap kejahatan dalam komunikasi. Seperti dapat terjadinya *scamming*, yang dimana *scamming* ini agak sulit untuk dihindari. Setiap orang bisa menerimanya apalagi jika pelaku *scamming* telah menentukan targetnya. Untuk itu, *user* perlu berhati-hati dalam mempercayai informasi dan melakukan konfirmasi pada pihak yang terkait. Dan ada juga yang namanya *spoofing* yang merupakan salah satu kejahatan dimana cara kerjanya adalah mengakses perangkat komputer, *email* dan akun lainnya dan pelaku akan berpura-pura menjadi pemilik akun yang asli. Pada *email* pelaku akan mengirimkan sebuah *email* dengan alamat pengirim yang palsu bertujuan untuk mencuri informasi yang dimiliki korban. Biasanya pelaku akan menyamar sebagai

teman, keluarga ataupun kolega kerja.

Kriptografi merupkan seni dan ilmu penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu data. Kriptografi juga tidak berarti hanya memberikan keamanan informasi saja, tetapi lebih ke arah teknik-tekniknya (Bhaudhayana dan Widiarta, 2015). Dalam menjaga kerahasiaan dan keamaan pesan elektronik (*Email*) tersebut maka penulis menggunakan metode algorithma enkripsi dan deskripsi yaitu *Revest Shamir Adleman* (RSA), agar data atau informasi tersebut dapat senantiasa terjaga kerahasiaan dan keamanannya dan juga RSA memiliki keamanan pada tingkat kesulitan dalam memfaktorkan bilangan non prima. Keamanan algoritma RSA adalah membuat pasangan kunci yaitu kunci publik dan kunci *private.* Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan yang dikirim dan diterima melalui *E-Mail*. Pesan-pesan tersebut dapat berupa data, atau informasi yang penting hanya boleh diketahui oleh si penerima pesan. Maka dari itu, untuk menjaga keamanan dan kerahasiaan pesan *e-mail* di perlukan perlindungan dengan membuat beberapa kode keamanan menggunakan kriptografi agar pesan yang dikirim tidak dapat dibaca atau dimengerti oleh sembarang orang. Dikarnakan di era saat ini masyarakan lebih sering menggunakan alat komunikasi yang mudah dibawa dan digunakan kapanpun dan dimanapun seperti penggunaan *smartphone*. Untuk Masyarakat Indonesia Lebih banyak menggunakan *smartphone* berbasis Android. Berdasarkan permasalahan di atas dibuatlah penelitian dengan judul "Perancangan Aplikasi Pengamanan Pesan Email Dengan Metode Kriptografi Rsa Berbasis Android Studio".

2. LANDASANTEORI

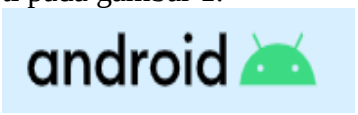
Elektronik Mail (E-Mail)

Menurut (Nugroho dkk, 2016), *Electronic Mail* (Surat Elektronik) adalah sebuah metode mengubah, mengirim, menyimpan, dan menerima pesan melalui sistem komunikasi elektronik. Istilah *e-mail* meliputi sistem yang berdasar pada *Simple Mail Transfer Protocol* (SMTP) dan sistem yang internet yang memungkinkan pengguna dalam satu organisasi mengirimkan pesan kepada satu sama lain. Seringkali kelompok orgranisasi tersebut menggunakan *internet protocol* sebagai layanan *e-mail* internal. Sebuah *e-mail* terdiri dari dua bagian besar yaitu:

1. Header :Berisi tentang informasi penting seperti alamat pengirim, alamat penerima, subjek dan tanggal.
2. Body : Bagian utama dari *e-mail* berisi text pesan, gambar, dan lainnya.

Android

Menurut (Juansyah, 2015), Android adalah sebuah sistem operasi perangkat *mobile* berbasis Linuc yang mencangkup sistem operasi, *middleware* dan aplikasi. Android menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka. *IoT* atau disebut dengan *internet of things* yaitu benda fisik yang terhubung dan dapat diakses dengan internet. Logo dapat dilihat seperti pada gambar 1.



Gambar 1. Logo Android (Android, 2021)

Android Studio

Menurut (Juansyah, 2015) Android Studio adalah IDE (*Integrate Development Environment*) resmi untuk membangun aplikasi android dan bersifat *oper source* atau gratis. Android studio sendiri dikembangkan berdasarkan *Intellij* IDEA yang mirip dengan *Eclipse* disertai dengan ADT *Plugin* (*Android Development Tools*). Android studio memiliki fitur :

1. Projek berbasis pada *Gradel Build*
2. *Refactory* dan pembenahan *bug* yang cepat.
3. *Tools* baru yang bernama "Lint" diklaim dapat memonitor kecepatan, kegunaan, serta kompetibelitas aplikasi dengan cepat.
4. Mendukung *Proguard And App-*Singung untuk keamanan.
5. Memiliki GUI aplikasi android lebih

mudah.

6. Didukung oleh *Google Cloud Platform* untuk setiap aplikasi yang dikembangkan.
   Logo dapat dilihat seperti pada gambar 2.

Gambar 2. Android Studio (Juansyah, 2015)

MySQL

Menurut (Mulana, 2016) MySQL adalah salah satu jenis *database server* yang sangat terkenal. Kepopulerannya disebabkan MySQL menggunakan SQL sebagai bahasa dasar untuk mengakses *database*-nya. MySQL, termasuk jenis RDBMS (*Relational Database Management System*). Pada MqSQL, sebuah *database* mengandung satu atau sejumlah *table. Table* terdiri dari atas sejumlah baris dan setiap baris mengandung satu atau beberapa kolom. Logo dapat dilihat seperti pada gambar 3.

Gambar 3. Logo MySQL (MySQL, 2021)

XAMPP

Menurut (Mawaddah dan Fauzi, 2018) XAMPP merupakan pengembangan dari LAMP (*Linux, Apache, MySQL, PHP and Perl).* XAMPP adalah *software web server web server apache* yang didalamnya tertanam *server* MySQL yang didukung dengan bahasa pemograman PHP untuk membuat *website* dinamis. XAMPP dapat berjalan pada berbagai macam *platform* seperti *Windows, Linux, Mac OS X,* dan *Solaris.*

Menurut (Putra, 2019) XAMPP merupakan *software server apache* dimana memiliki banyak keuntungan sepeti mudah untuk digunakan, tidak memerlukan biaya serta mendukung pada isntalasi *windows* dan *linux.* Hal ini juga didukung karena instalasi yang dilakukan satu kalo tersedia MySQL, *apache web server, database server* PHP *support.* Logo dapat dilihat seperti pada gambar 4.

Gambar 4. Logo XAMPP(XAMPP, 2021)

Kriptografi

Menurut (Ginting dkk, 2015) Kriptografi (*Cryptography*) berasal dari bahasa yunani yang terdiri dari kara *kryptos* yang artinya tersembunyi dan *graphia* yang artinya sesuatu yang tertulus sehingga kriptografi dapat juga disebut sebagai sesuatu yang tertulis secara rahasia atau tersembunyi. Menurut terminiloginya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain.

Dalam kriptografi, pesan atau informasi yang dapat dibaca disebut sebagai *plaintext* atau *clear text.* Proses yang dilakukan untuk mengubah teks asli (*plaintext*) ke dalam teks rahasia (*chipertext*) disebut enkripsi. Pesan yang tidak terbaca disebut teks rahasia (*chipertext*). Proses kebalikan dari enkripsi disebut deskripsi. Deskripsi akan mengembalikan teks rahasia menjadi teks asli. Kedua proses enkripsi dan deskripsi membutuhkan penggunaan sejumlah informasi rahasia, yang sering disebut kunci (*key*).

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1. Kerahasiaan
   Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang

memiliki otoritas untuk membuka informasi yang telah disandi.

2. Integritas Data

Integritas adalah berhubungan dangan penjaan dari perubahan data secara tidak sah.

3. Autentikasi

Autentikasi adalah berhubungan identufukasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri.

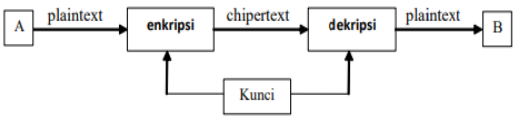
4. Non-repudasi atau Nirpenyangkalan

Non-repudasi atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan atau membuat.

Menurut (Himawan dkk, 2016) Dalam perkembangannya algoritma kriptogradi terbagi menjadi dua macam yaitu:

1. Algortima Simetris

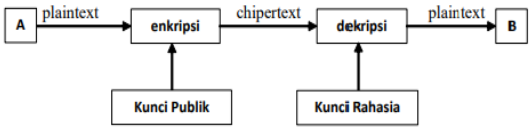
Algoritma simetris adalah jenis algoritma kriptogradi yang dalam proses enkripsi dan deskripsi menggunakan kunci yang sama. Algoritma ini mengharuskan pengirim dan penerima menentukan suatu kunci tertentu sebelum melakukan komunikasi. Keamanan algoritma simetris tergantung pada kunci tersebutm membocorkan kunci berarti orang lain dapat mengenkripsi dan mendeskripsi pesan. Alur algotirma simetris dapat dilihat pada gambar 5.



Gambar 5 Algoritma Simetris (Himawan dkk, 2016)

2. Algoritma Asimetris

Algoritma Asimetris atau yang sering disebut dengan algoritma kunci publik menggunakan dua jenis kunci yaitu, kunci publik dan kunci rahasia. Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan dan bersifat umum, sehingga dapat diketahui oleh siapa saja. Sedangkan kunci rahasia digunakan untuk mendeskripsi pesan dan bersifat rahasia, sehingga hanya diketahui oleh orang yang memiliki otoritas. Alur algoritma asimetris dapat dilihat pada gambar 6.



Gambar 6. Algoritma Asimetris (Himawan dkk, 2016)

Algoritma RSA (*Rivest Shamir Adleman*)

Menurut (Rizkyansyah dan Saifudin, 2018) Pada bidang kriptografi, RSA merupakan sebuah algoritma enkripsi yang menggunakan kunci publik. RSA adalah algoritma pertama yang sesuai dengan *digital signature* seperti halnya eknripsi, dan menjadi salah satu algoritma yang paling maju dalam bidang kriptografi kunci publik. RSA telah digunakan secara luas pada *protocol electronic commerce*, dan dipercaya untuk mengamankan data menggunakan kunci yang cukup panjang. RSA merupakan algoritma kunci publik yang paling popular dari algoritma yang pernah dibuat.

Algoritma RSA dikembangkang pada tahuin 1976 oleh 3 orang peneliti dari MIT (*Massachussets Institute of Technology*), yaitu Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor bilangan prima merupakan kunci keamanan algoritma RSA. Pemfaktoran digunakan untuk mendapatkan kunci pribadi. Selama pemfaktoran bilang dengan nilai yang besar menjadi-faktor prima belum ditemukan, maka selama itu pula keamanan algoritma RSA terjamin.

Proses Enkripsi RSA

Menurut (Ginting dkk, 2015) Langkah-langkah pada proses enkripsi algoritma RSA sebagai berikut :

1. *Plaintext* diubah kedalam bentuk bilangan. Untuk mengubah *plaintext* yang berupa huruf menjadi bilangan dapat menggunakan kode ASCII dalah sistem bilangan desimal.

2. *Plaintext* m dinyatakan menjadi blok-blok x1,x2,x3,…, sedemikian sehingga setiap blok merepresentasikan nilai didalam selang [0, n-1], sehingga transformasinya menjadi satu ke satu.
3. Setiap blok mi dienkripsi menjadi blok c_i dengan rumus :

$$y_i = x_i^{PK} \bmod r$$

Proses Deskripsi RSA

Menurut (Ginting dkk, 2015) Langkah-langkah pada proses deskrisi algoritma RSA sebagai berikut :

1. Setiap blik *chipertext* y_i dideskripsi kembali menjadi blox x_i dengan rumus

$$x_i = y_i^{SK} \bmod r$$

2. Kemdian blok-blok m1,m2,m3,…, diubah kembali ke bentuk huruf dengan melihat kode ASCII hasil deskripsi.

Pengujian

Menurut (Mustaqbal dkk, 2015), pengujian adalah suatu proses pelaksanaan suatu program dengan tujuan menemukan suatu kesalahan. Suatu kasus test yang baik apabila test tersebut mempunyai kemungkinan menemukan sebuah kesalahan yang tidak terungkap.

User Acceptance Testing

Menurut (Nurdin dan Hermawan), *User Accaptance Text* (UAT) atau uji penerimaan pengguna adalah suatu proses pengujian oleh pengguna yang dimaksudkan untuk menghasilkan dokumen yang dijadikan bukti bahwa *software* yang telah dikembangkan telah dapat diterima oleh pengguna, apabila hasil pengujian (*testing*) sudah bisa dianggap memenuhi kebutuhan dari pengguna.

Black Box Testing

Menurut (Mustaqbal dkk, 2015), *Black Box Testing* berfokus pada spesifikasi fungsional dari perangkat lunak. *Tester* dapat mendefinisikan kumpulan kondisi *input* dan melakukan pengetesan pada spesifikasi fungsional program. *Black box testing* cenderung untuk menemukan hal-hal berikut:

1. Fungsi yang tidak benar atau tidak ada.
2. Kesalahan antar muka (*interface errors*).
3. Kesalahan performansi (*performance errors*).

Skala *Likert*

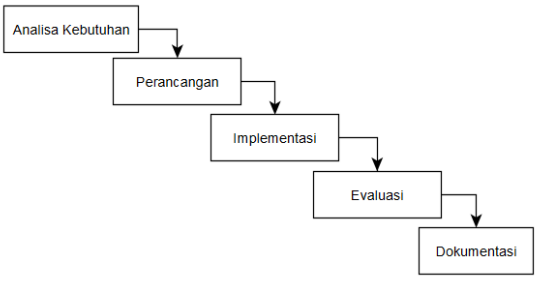
Menurut (Bahrun dkk, 2017), Skala *likert* adalah skala yang digunakan dalam mengukur sikap, pendapat, dan persepsi seseorang atau orang tentang fenomena sosial. Dengan skala *likert*, maka variabel yang ada diukur dijabarkan menjadi indikator variabel. Kemudian indikator tersebut dijadikan titik tolak untuk menyusun item-item *instrument* yang dapat berupa pernyataan atau pertanyaan.

Karakteristik dari skala ini yang membedakannya dari skala lain adalah pilihan dari masing-masing pertanyaan dari *instrument* yang digunakan berupa pilihan dari masing-masing pertanyaan dari *instrument* yang digunakan berupa pilihan yang mempunyai gradasi dari sangat posotif sampai dengan negatif. Seperti sangat setuju, ragu-ragu, tidak setuju, dan sangat tidak setuju. Dalam skala *likert* bentuk penyajian yang dapat digunakan terbagi menjadi dua pilihan yaitu pilihan ganda dan bentuk *checklist.*

3. METODE PENELITIAN

Alur Penelitian

Adapun alur penelitian pada pembuatan aplikasi ini bisa dilihat pada gambar 6 berikut ini:



Gambar 6. Alur Penelitian

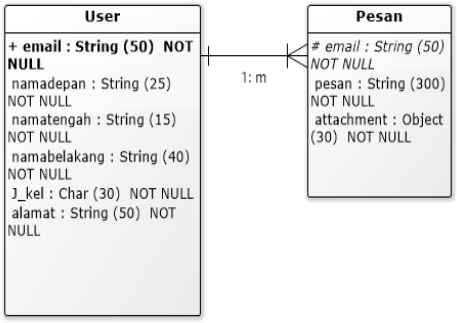
1. Fase Pengumpulan Kebutuhan

Pada tahap ini peneliti dan pengguna bersama-sama mendefinisikan format dan kebutujan perangkat lunak dan garis besar sistem yang akan dibuat.

2. Fase Perancangan

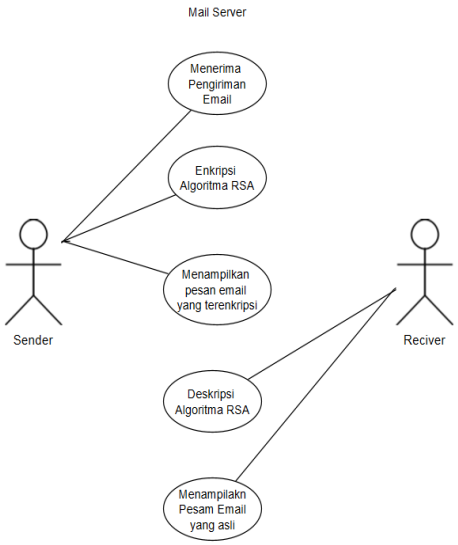
Pada tahap ini perancangan atau membangun *prototyping* ini pengembang memulai membuat rancangan sistem yang akan dibuat seperti oerancangan diagram sistem yang akan dibuat, dan database yang dibutuhkan.

Berikut perancangan Database menggunakan ERD :



Gambar 7. Perancangan Database menggunakan ERD

Berikut adalah perancangan *use case* diagram :



Gambar 8. Perancangan Use case Diagram

3. Fase Implementasi

Pada fase ini pengembang mengimplementasikan semua rancangan *prototype* dan database menjadi sebuah aplikasi yang dapat digunakan.

4. Fase Evaluasi

Pada tahap ini pengguna aplikasi akan mengevaluasi *prototype* yang dibuat dan mengevaluasi hasil kerja dari perancangan sistem yang telah dibuat. Pada tahap ini akan dilakukan proses pengujian atas kebutuhan sistem yang telah di rencanakan sebelumnya.

5. Fase Dokumentasi

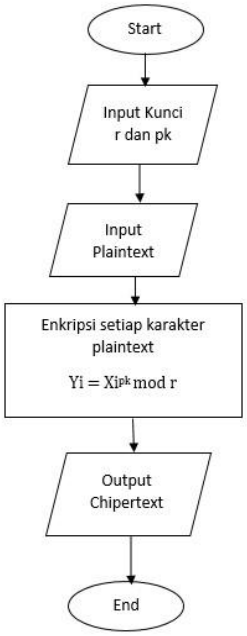
Pada tahap ini dilakukan semua proses dokumentasi atas apa yang sudah dikerjakan selama proses penelitian, pembuatan kesimpulan dan saran dari penelitian yang sudah diselesaikan.

Alat Penelitian

Pada penelitian pengembangan ini alat penelitian yang dibutuhkan adalah Personal komputer untuk mengirimkan pesan *emai* yang terenkripsi, *server* komputer untuk mengolah dan menyimpan data *email client*, modem dan beberapa perangakat jaringan.

Proses Enkripsi RSA

Alur proses enkripsi RSA dapat dilihat pada gambar 9.

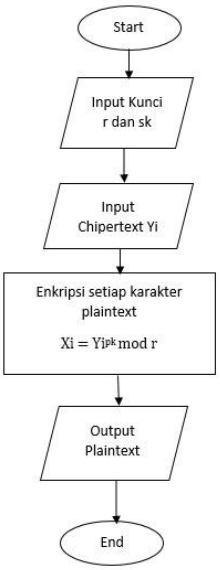


Gambar 9. Diagram Flowchat Enkripsi RSA

Alur diagram flowchat enkripsi RSA, *Input* kunci r dan pk (kunci publik) lalu *input plaintext*. Setelah plaintext ter-*input* baru bisa memulai enkripsi. Enkripsi dilakukan mennggunakan rumus yang tertera pada gambar 9. Setelah terenkripsi maka menghasilkan *output* berupa *chipertext*.

Proses Deskripsi RSA

Alur proses enkripsi RSA dapat dilihat pada gambar 10.



Gambar 10. Diagram Flowchat Deskripsi RSA

Sedangkan Alur deskripsi RSA, menggunakan inputan sk (kunci privte) dan Chiphertext. Setelah chipertext ter-input baru bisa melakukan deskripsi menggunakan rumus yang tertera pada diagram 3.5 dan menghasilkan output berupa plaintext.

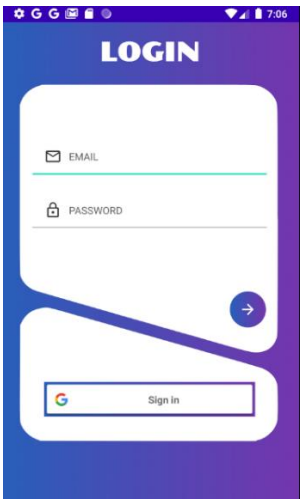
4. HASIL DAN PEMBAHASAN

Implementasi Tampilan Aplikasi Krasa

Berikut adalah implementasi tampilan dari aplikasi Krasa :

1. Tampilan *Login*

Impelementasi tampilan *login* berdasarkan rangcangan yang telah dibuat akan dijelaskan pada gambar 11.

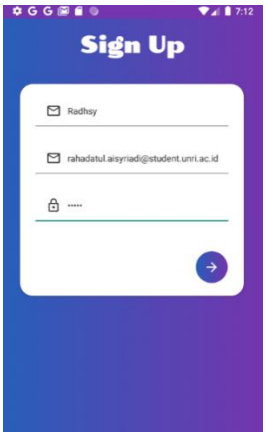


Gambar 11. Tampilan Menu *Login*

Untuk masuk kedalam aplikasi, pengguna diminta untuk melakukan login terlebih dahulu. Untuk pengguna yang sudah terdaftar bisa langsung mengisi alamat *e-mail* dan *password*. Apabila pengguna belum terdaftar bisa bisa meng-klik tombol *sign in* yang tertera di tampilan aplikasi.

2. Tampilan Sign Up

Impelementasi tampilan *sign up* berdasarkan rangcangan yang telah dibuat akan dijelaskan pada gambar 12.



Gambar 12. Tampilan *Sign Up*

Setelah *Sign In* menggunakan Gmail, barulah pengguna melakukan *sign up* untuk aplikasi Krasa. Dengan cara mengisi nama, alamat *email* dan *password*.

3. Tampilan Menu Utama

Impelementasi tampilan Menu Utama berdasarkan rangcangan yang telah dibuat akan dijelaskan pada gambar 13.

Gambar 13. Tampilan Menu Utama

Tampilan menu utama berisi dengan semua *email* masuk yang isi pesannya telah terenkripsi. Untuk dapat membaca pesanya maka pengguna harus membuka isi *email* tersebut. Dan untuk mengirim pesan ke pengguna lain, pengguna bisa meng-klik tombol (+) atau *compose*.

4. Tampilan *Compose*

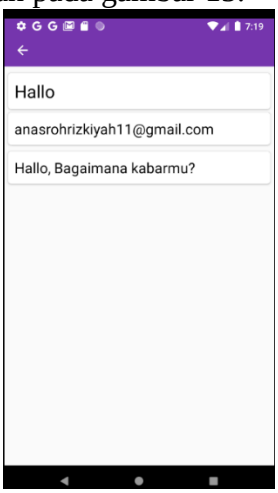
Impelementasi tampilan *Compose* berdasarkan rangcangan yang telah dibuat akan dijelaskan pada gambar 14.

Gambar 14. Tampilan Menu *Compose*

Tampilan menu *Compose* terdiri dari *from, to, subject,* dan *messege*. Pada kolom *from,* alamat *email* penggunaka akan langsung tertera. Lalu pada kolom *to,* pengguna bisa mengisi alamat *email* yang dituju. Untuk kolom *subject,* pengguna bisa mengisikan subjek dari *email* yang akan dikirimkan. Dan untuk kolom *messege,* pengguna bisi menulikan isi pesan yang ingin dikirimkan. Setelah semuanya terisi pengguna bisa langsung mengirimkan pesan dengan cara menekan tombol *sent*.

5. Tampilan Isi Pesan

Impelementasi tampilan Isi Pesan berdasarkan rangcangan yang telah dibuat akan dijelaskan pada gambar 15.



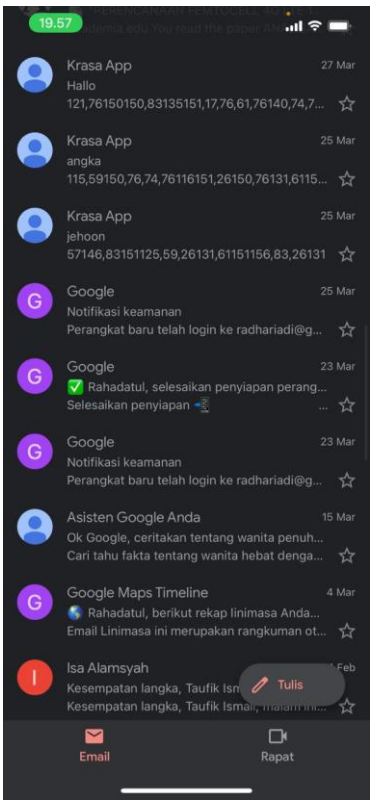
Gambar 15. Tampilan Menu Isi Pesan

Tampilan menu isi pesan, berisi pesan yang telah di deskripsi sehingga pengguna bisa membaca isi pesan tersebut.

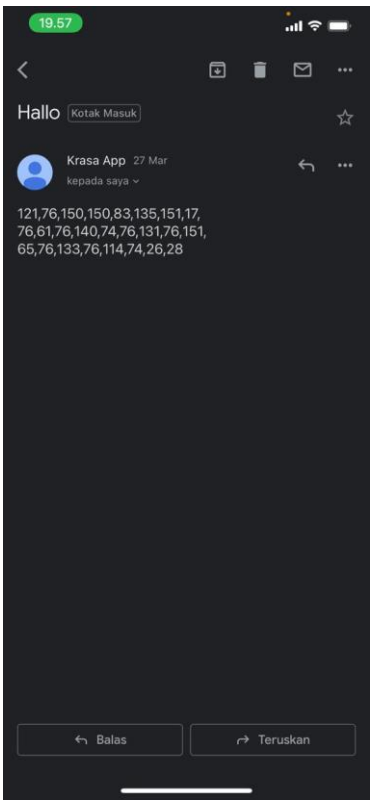
Berikut adalah implementasi tampilan yang diterima di Gmail:

1. Tampilan Pesan yang Diterima

Berikut tampilan dari pesan yang diterima sesuai dengan rancangan yang telah dibuat.



Gambar 16. Tampilan Menu Isi Pesan



Gambar 17. Tampilan Menu Isi Pesan

Tampilan menu pesan yang diterima, berisi pesan atau *e-mail* yang telah diterima oleh pengguna, baik dari aplikasi Krasa maupun dari *e-mail* yang lain.

2. Tampilan Isi Pesan yang Diterima

Berikut tampilan dari isi pesan yang diterima sesuai dengan rancangan yang telah dibuat.

Tampilan menu isi pesan yang diterima, berisi pesan yang telah terenkripsi. Isi pesan berupa angka-angka atau bilangan dan jika pengguna ingin membaca isi pesan tersebut bisa melalui aplikasi Krasa.

Hasil Pengujian Sistem Keseluruhan

Tujuan dari pengujian ini adalah untuk mengukur kemudahan penggunaan dari aplikasi Krasa. Pengujian ini dilakukan dengan cara mengamati interaksi pengguna dengan aplikasi android berdasarkan pilihan jawaban dari responden.

User Acceptance Testing

Tujuan dari pengujian ini adalah untuk mengukur kemudahan penggunaan aplikasi Krasa. Berikut ini adalah hasil pengujian yang telah dilakukan kepada 15 responden. Pengujian ini dilakukan dengan cara menjawab 9 pertanyaan yang dilengkapi dengan 5 jawabab “Sangat Mudah”. “Mudah”, “Cukup Mudah”, “Sulit”, dan “Sangat Sulit”. Hasil uji dapat dilihat pada tabel 1:

Tabel 1 Indikator Pengujian Pada aplikasi Krasa dengan 15 responden

No	Pertanyaan	Jawaban					Total Skor Responden (nl+...+nz = f)	Persentase Skor/item $\frac{f}{10}$ x 100
		S M	M	C	S	SS		
Aspek Tampilan Aplikasi Konsultasi untuk Dokter								
1.	Bagaimana pendapat pengguna mengenai tampilan *desain* aplikasi Krasa	0	8	7	0	0	53	70.6%
2.	Bagaimana pendapat pengguna mengenai pemilihan warna pada aplikasi Krasa?	0	8	7	0	0	53	70.6%
Aspek Kegunaan dan Manfaat Aplikasi Krasa								
1.	Apakah pengguna berhasil melakukan *login* menggunakan aplikasi?	5	7	3	0	0	62	82.6%
2.	Apakah pengguna berhasil dalam melakukan *sign up*?	3	8	4	0	0	59	78.6%
3.	Apakah pengguna dapat menjalankan aplikasi dengan mudah?	4	6	5	0	0	59	78.6%
4.	Apakah fitur-fitur yang ada di dalam aplikasi dapat dijalankan dengan mudah?	6	5	4	0	0	62	82.6%
5.	Apakah pengguna dapat mengirimkan pesan dengan mudah menggunakan aplikasi Krasa?	4	7	4	0	0	60	80%
6.	Apakaj pengguna dapat membaca isi pesan dengan mudah saat menggunakan aplikasi Krasa?	5	4	6	0	0	59	78.6%
7.	Apakah apliasi Krasa bermanfaat bagi pengguna?	5	5	5	0	0	57	76%
Total nilai maksimal persentase peritem adalah 9 x 100 = 900 Total = $\frac{\text{Jumlah persentase skor}}{900}$ x 100								77.8%

Berdasarkan table 1 didapat rata-rata persentase likert Krasa dapat layak digunakan 77,8% dari 15 responden. Maka dapat disimpulkan bahwa aplikasi.

Black Box Testing

Berikut ini adalah hasil dari pengujian yang telah dilakukan oleh responden.

Tabel 2 Indikator Pengujian Pada aplikasi Krasa dengan 15 responden

No	Pengujian	Aksi	Hasil yang Diharapkan	Hasil Uji
1	Tombol *login* pada tampilan *login*	Klik	Menyeleksi pengguna yang masuk ke dalam sistem	Sesuai
2	Tombol *Sign in* via Gmail pada halaman *Login*	Klik	Menampilkan halaman penambahan akun dengan Gmail	Sesuai
3	Tombol *Next* atau tombol masuk pada halaman *Sign up*	Klik	Menyeleksi pengguna yang masuk ke dalam sistem	Sesuai
4	Tombol tambah pada halaman utama	Klik	Menampilakan halaman *compose* untuk mengirim pesan	Sesuai
5	Tombol Kirim pada halamam *Compose*	Klik	Untuk mengirimkan pesan	Sesuai
6	Tombol *back* pada halaman *compose*	Klik	Menampilkan Kembali menu utama	Sesuai
7	*List* pesan masuk pada halaman menu utama	Klik	Menampilkan isi pesan yang diterima	Sesuai
8	Tombol *Exit* pada halaman utama	Klik	Menampilkan Kembali pada halaman *Login*	Sesuai

Berdasarkan tabel 2 hasil uji coba, dapat disimpulkan bahwa aplikasi Krasa sudah sesuai dengan kriteria yang telah ditetapkan.

5. KESIMPULAN DAN SARAN

Kesimpulan

Adapun kesimpulan dari penelitian "Perancangan Aplikasi Pengamanan Pesan E-Mail Dengan Metode Kriptografi RSA Berbasis Android Studio" adalah sebagai berikut :

1. Aplikasi Krasa ini hanya bisa digunakan oleh pengguna yang telah terdaftar atau *sign up* dan peengguna hanya bisa berkomunikasi atau mengirim pesan satu sama lain dengan sesama pengguna aplikasi Krasa.
2. Untuk dapat membaca isi pesan yang telah di deskripsi hanya bisa melalui aplikasi Krasa.
3. Berdasarkan hasil uji dari aplikasi krasa menggunakan pengujian *user acceptance testing* dengan metode perhitungan skala likert menunjukkan bahwa aplikasi dinyatakan mudah dan layak untuk digunakan.
4. Pengujian aplikasi pada 15 responden menggunakan pengujian *black box* menunjukkan bahwa aplikasi telah sesuai.

Saran

Adapun saran untuk penelitian selanjutnya adalah aplikasi Krasa ini dapat berjalan di system operasi IOS dan juga bisa ditambahkan fitur-fitur baru seperti menambahakan pilihan untuk mengirim pesan berupa *file* atau *attachment* dan lainnya.

DAFTAR PUSTAKA

Albert Ginting, R. Rizal Isnanto, Ike Pertiwi Windasari, 2015, Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email, Jurnal Teknologi dan Sistem Komputer, Vol. 3 No.2, April 2015

Bahrum, Suryadi dkk. 2017. Rancan Bangun Sistem Informasi Survey Pemasaran dan Penjualan Berbasis Web. Jurnal Transistor Elektro dan Informatika (TRANSISTOR EI) Vol. 2, No. 2, Oktober 2017, pp. 81~88.

Himawan, Cindy dkk. 2016. Studi Perbandingan Algoritma RSA dan Algoritma El-Gamal. Lombok: Seminar Nasional APTIKOM (SEMNASTIKOM)

Juansyah, Andi. 2015. Pembangunan Aplikasi Child Tracker Berbasis Assisted-Global Positioning System (A-GPS) dengan Platform Android. Bandung: Edisi. 1 Volume. 1 Agustus 2015 ISSN : 2089-9033

Lesmana, Andrian dkk. 2018. *Aplikasi Pengamanan Email Berbasis Android Dengan Algoritma Kriptografi AES-128 dan RC4 pada PT Tirta Investama*. Jakarta: Skanika Volume 1 No. 2 Mei 2018

Maulana, Halim. 2016. Analisis dan Perancangan Sistem Replikasi Database MySQL dengan Menggunakan VmWare pada Sistem Operasi Open Source. Medan : InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan) e-ISSN : 2540-7600 Vol 1, No 1, September 2016 p-ISSN : 2540-7597

Mawaddah, Udkhiati, Muchtar Fauzi. 2018. Sistem Pendukung Keputusan Untuk Menentukan Dosis Obat pada Anak Menggunakan Metode Forward Chainig (Studi Kasus di Klinik Dokter Umum Karangayam-Srengat). Jurnal Antivirus, Vol. 12 No. 1 Mei 2018 p-ISSN: 1978-5232 e-ISSN: 2527-337X.

Mustaqbal, M Sidi dkk. 2015. Pengujian Aplikasi Menggunakan Black Box Testing Boundary Value Analysis (Studi Kasus : Aplikasi Prediksi Kelulusan SNMPTN). Bandung. Jurnal Ilmiah Teknologi Informasi Terapan Volume I, No 3.

Nugroho, Nurcahyo Budi dkk. 2016. Aplikasi Keamanan Email Menggunakan Algoritma RC4. Jurnal SAINTIKOM Vol.15, No. 3

Putra, Agustiranda Bagaskara. 2019. Perancangan dan Pembangunan Sistem Informasi E-Learning Berbasis Web (Studi Kasus Madrasah Aliyah Kare Madiun). Madiun: e-ISSN: 2685-5615